Edith Cowan University
Research Online

Australian Information Warfare and Security Conference

Security Research Institute Conferences

2006

Information terrorism: networked influence

W Hutchinson
Edith Cowan University

Originally published in the Proceedings of 7th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 4th - 5th December, 2006.
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/isw/10

Information terrorism: networked influence

W. Hutchinson
School of Computer and Information Science
Edith Cowan University
Email: w.hutchinson@ecu.edu.au

Abstract

The advent of digital information technology heralded the concept of information warfare. This 'preliminary' stage in the 1990s really consisted of technology warfare where the networks, upon which combat relied, were seen as weapons to gain 'information superiority'. This was the inception of the technological aspect of Information Warfare. The realisation of the effectiveness of electronic networks to optimize organisational communication was taken up by industry, the military and terrorist groups alike. As society quickly became more reliant on digital networks to run its critical functions, it became apparent that this infrastructure was vulnerable and needed protection (as well as being a target for offensive operations).The next stage was the emphasis not on the technology but the information which it stored and processed. This was the 'information' stage of Information Warfare (now renamed Information Operations to reflect its expanded scope). This stage developed further and gradually started to include elements such as public relations, and strategic communications This paper examines the development of these elements and their use by terrorist groups. It concentrates on the contemporary manifestations of Influence Wars.

Keywords

Information Operations, Information Terrorism, Influence Campaigns, Psychological Warfare.

THE 'NEW' ENVIRONMENT

There is general agreement that the 'new' form of trans-national terrorism has change the complexion of terrorism in the last decade. The main trends pertaining to these trans-national groups are:

- The development of loose networks / *ad hoc* groups as the preferred *modus operandi*;
- A new attitude towards violence including suicide bombing;
- Religious based groups rather than nationalistic;
- Operations facilitated by Information and Communications Technologies (ICT) and mobile technologies;
- Ideas and worldviews bind them together rather than just political aspirations;
- They have less need for direct state sponsorship;
- Groups appeal to diasporas rather than just domestic audiences; and
- They have the potential to use Chemical, Biological, Radiological and Nuclear weapons.

(Arquilla *et al*., 1999; Hoffman, 1998, 1999; Medhurst, 2002)

In the era of globalization, terrorism itself has been globalized. The 'new' terrorist organisations are loosely organized into groups that have some centrally espoused worldview (such as *Al Qaeda*) but not necessarily a centralised organisational structure. There is a trend towards religious based groups rather than nationalistic, and these group tend to be much more lethal. In fact, all trans-national groups are religious in nature. Because of their religious /cultural focus they tend to get support from sympathisers in religious/ethnic communities in disparate countries. These are mostly first or second generation immigrants in Western nations although there is still a core of support in the countries of origin. At this time, the major globalised religious groups are based around radical Islam. The advent since the early 1990s of global communications and mass media has empowered these groups to use these media as tools for command and control, collections of funds, and also

importantly to provide them with a worldwide audience for their views. For instance, the low cost of Internet web pages enables terrorist groups to publish material to a global audience. In fact, in the early 1990s, terrorist groups of all kinds were the first to fully exploit this developing medium. The evolution of the use of these technologies developed in tandem with their use by Western government and militaries.

INFORMATION TERRORISM

The concept of *information terrorism* has its origins in the ideas that surrounded *information warfare*. Libicki (1995) first described the elements of information warfare to be seven subtypes of warfare: Command and Control, Intelligence Based, Hacker, Electronic, Psychological, Cyber and Economic based information warfare. Information warfare in its early stages was very much focused on exploiting the new technologies to gain advantage. Whilst there was an element of psychological warfare, it was predominantly about command and control and disruption of enemy systems. As the potential of these technologies to influence both friend and foe was realised, there was a renewed focus on this aspect. As the wars of the late 1990s' became more politicised, the advantage of information dominance (or information superiority), began to be recognised and were used in both times of 'peace' and 'war' – as the distinction between these two states faded. The term Information Operations was coined to superseded the more dramatic information warfare (which is now a sub-set of information operations to be used in times of open conflict).

In this paper *Information terrorism* is defined as the practice of information operations by those deemed to be terrorists. Figure 1 illustrates some of the elements of information operations/ information terrorism.

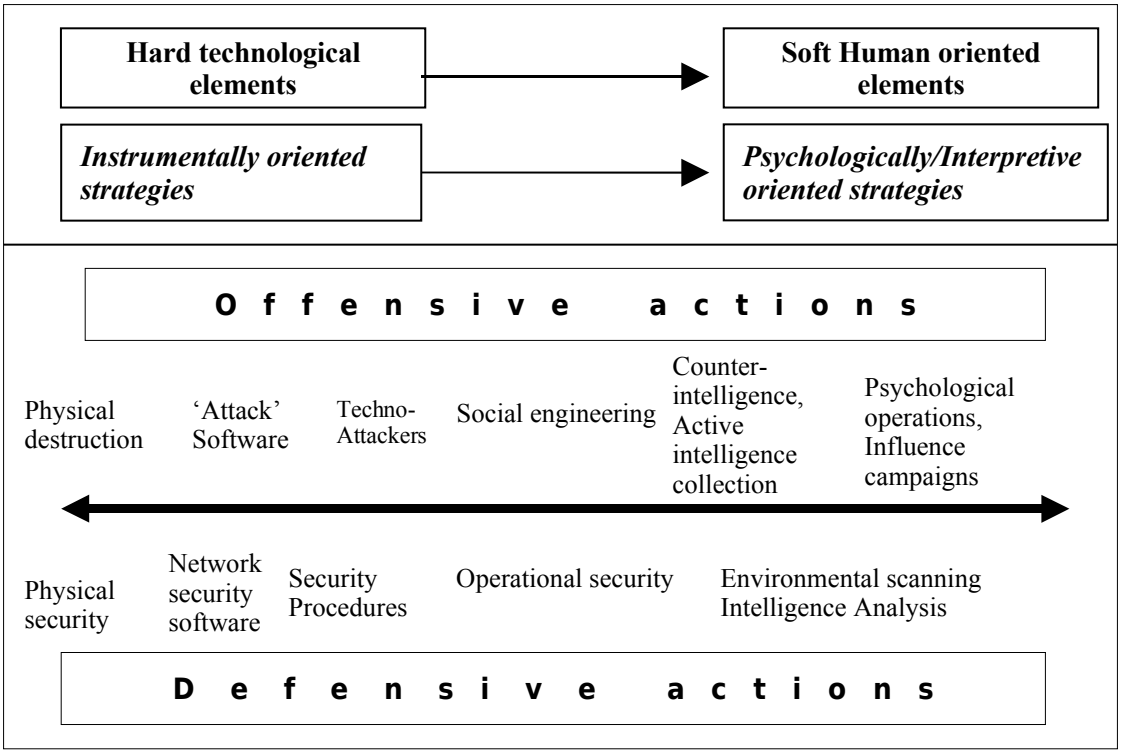

Figure 1: Examples of the Elements of Information Operations/Terrorism

It can be seen from Figure 1 that information terrorism consists of a variety of components ranging from technology (instrumentally) based approaches to human (psychologically) based activities. In a way, this describes the development of the emphasis of information operations over the last two decades. It has both defensive and offensive modes. This paper concentrates on the human/psychologically oriented offensive strategies used by terrorist groups. Information Operations (IO) has developed into a truly Information/Knowledge Age phenomenon, as Hall (2003, p.97) illustrates:

> *Information operations of the future will rely on both a philosophy and a set of tools. The philosophy of IO acknowledges the emergence and importance of knowledge war and its direct connection to knowledge-based strategies and knowledge-based operations. The philosophy acknowledges the pre-eminence of information and knowledge as they contribute to effective decision making, as well as the importance of thinking planning and perceptions from two points of view: ours and the adversary's. The IO suite of tools will be used to attack the thinking, planning, decision-making processes, the*

mechanical turning of data into information and information into knowledge, and the machinery supporting the decision making cycles of our adversaries.

Whilst this is written from a conventional military perspective, it captures the essence of the use of information operations by terrorists and government agencies in conflict with them.

Table 1 outlines some of the components of contemporary information terrorism. Whilst there are a number of Command and Control and Cyber war elements, it is the Influence functions components that dominate.

Table 1: Contemporary factors influencing Information Terrorism

CYBERWAR FUNCTIONS:

- **Attack technology by using:**
  - ✓ *Logic bombs, viruses, worms, spy-ware, flooding, DOS attacks, Web defacement*
- **Defend technology by using:**
  - ✓ *Virus checkers, network tools, network forensics, standards, backups, intrusion detection systems, honeypots, training*

ORGANISATIONAL (COMMAND AND CONTROL) FUNCTIONS:

- **Coordinating activities:**
  - ✓ *Network centric organisations using such elements as the Web, SMS, coordinated sensors, and streaming video.*
- **Bind supporters and spread message:**
  - ✓ *Use the Web and the mass media to promote cause to a global audience. Use the Web to collect monies.*

MIND/INFLUENCE FUNCTIONS:

- **Contemporary audience**
  - ✓ *Globalized reach of communications has given the ability to reach anyone/anywhere.*
- **Strategic communications**
  - ✓ *Influence campaigns are now an integral part of national and terrorist strategy. Each has its own targeted constituency in the globalized information environment.*
- **Terrorism is psychological warfare**
  - ✓ *Violence as communication.*
  - ✓ *Goals cannot be obtained by violence alone.*
  - ✓ *Victims must be enlisted to gain objectives.*
  - ✓ *Persistent campaign with the target population increasingly perceiving (irrationally?) risk.*
  - ✓ *Boost its supporters, frighten it opponents.*
  - ✓ *Seek to undermine beliefs in the collective values of society.*
  - ✓ *Terrorists uses the victims' imagination against themselves*
- **Technology of the despised West is used against it**
  - ✓ *Even the Taliban, who are averse to technology, had a Web site.*
  - ✓ *Web and other technologies such as SMS are more difficult to censor.*
  - ✓ *Terrorists' Web sites are better suited to their target audiences than 'official' sites.*
  - ✓ *Effective use of video imagery on Web and, subsequently, the mass media.*
- **Technology has decreased the West's dominance of mass communication.**
  - ✓ *The terrorists' strategy is recognises the importance of having information/influence practices.*
  - ✓ *The importance of the media is shown by the increase in violent targeting of broadcasters by Western militaries and governments*
  - ✓ *Censorship of the Web is increasing although terrorists seem to be able to combat this*

It is the Mind/Influence functions that will be further discussed below.

INFLUENCE OPERATIONS AND TERRORIST GROUPS

Terrorism can predominantly be considered as asymmetric warfare fought mostly as psychological warfare. *Psychological warfare* is a term used to describe the suite of actions that consists of violence or the threat of violence plus some form of psychological operations. Psychological operations consist of actions such as disinformation, deception, propaganda, and showing force (Goldstein and Jacobowitz, 1996). In its most successful form, it can create a victory without the need to use force. Traditionally, it has been considered another way of making the enemy surrender. However, its tactics can be used to both destroy the 'will' of the

enemy, and boost the 'will' of supporters. In contemporary terrorist actions the actors are the terrorists themselves, their supporters, those that are neutral, plus governments and global publics. Terrorists know that they cannot win using violence alone as, militarily, they are in a weaker position.

The violent components of terrorist actions are symbolic and designed to send a (political) message (Tuman, 2003). In a sense, if there was no message to be understood by the targeted audience then such things as bombings and shootings would have no objective except violence itself. Although certain religious based terrorist groups do seem to want to maximise body counts (Medhurst, 2002), there is still an underlying political message. Tuman (2003, pp. 46-48) states that symbolic acts of violence should be analysed using the following factors: the intent of the communication, the context of the communication, and the relativity of the symbolic message. Each of these acts of violence has primary, secondary, and tertiary targets or audiences. For instance the attacks on September 11th, 2001 on New York and Washington had the immediate target of the victims of the violence, secondary targets such as the American government and public and the global Islamic population, and tertiary audiences in Europe and other countries. The symbolism of the attacks and their targets were numerous; they were attacks on the US military (the Pentagon), its government (the failed attempts on the Whitehouse /Capitol), and the capitalist economic/trading systems (the World Trade Centre). Also, it could be considered an attack on the invulnerability of the American 'homeland', and modernity (represented by the architecture of the World Trade Centre).

However, these attacks are the determinants of whether a group is considered to be a terrorist group or not: much of the influence effort goes around these events. The acts of violence by themselves are almost meaningless without messages and context. Whilst the violence is a form of messaging, the underlying political/religious objectives of these acts need to be communicated. Hence, each message must have a context, and intent, and a targeted audience. The latter might involves varies degrees of impact depending on the audience targeted.

Also, there is a need for the terrorists to target various stages of influence in their desired audiences. For instance, radical Islamists desire long term goals and, as such, temporary disturbances that will be forgotten in a short period might be tactically beneficial to them but must be a part of a longer term strategic plan. Figure 2 explains the types of influence, their relative gestation period and their outcomes.

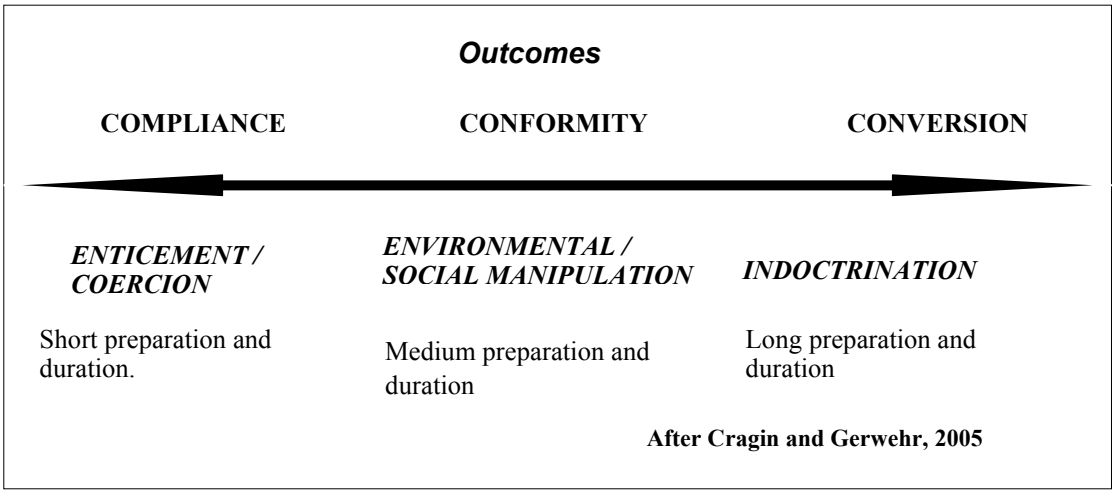

Figure 2: Elements of Strategic Influence /Psychological Operations

The short term tactics of enticement and coercion are really a classic psychological warfare method. Compliance might be obtained but belief systems are not altered. So whilst intimidation might provide short term changes in behaviour, the underlying political message has not necessarily been accepted by the target audience. The next step to obtain conformity in the target audience is more difficult to achieve. Inducements such as peer pressure, and the credibility of the message and presenter assist in bringing about this medium term goal (Cragin and Gerwehr, 2005, pp.17-19). For terrorist groups, this outcome can realised in areas where the message has some context. For instance, for Islamic terrorist groups, in regions with a high proportion of Muslims. Once the social context has been controlled, the next long term step is to progress to the conversion stage where the audience is more or less controlled by the influencer. Religious schools or tightly controlled states produce this long term outcome, and fewer inducements have to be given relative to the changes in the other two stages.

The campaign by *Al Qaeda* can be seen in this light. The first stage was highlighted by spectacular violent events that brought short term visibility, and targeted the Muslim *ummah*. This stage showed

the West being coerced and sent out the message that the oppression of Muslim by the West was being fought by *Al Qaeda*. Reactions by the West and the social consequences that this caused in Iraq, Afghanistan, Palestine, and other areas such a Chechnya created a social and political environment that was conducive to conversion, or partial conversion, of Muslims to *Al Qaeda's* cause. In certain areas, this process has radicalised portions of the Islamic population and encouraged the development of radical Islamic schools or *maddrasses*.

Persuasive communication must go through a series of steps before it is transformed into action. Firstly, the audience must be exposed to the message. In terms of successful terrorist groups, this is usually achieved by some spectacular act of violence that it relayed through the mass media and then followed up by Web page entries. Sometimes the event is transmitted through the Web first and then picked up by the media, for instance, beheadings of hostages in the 2002 - 2005 period. The message must then receive attention by the audience: that is, it must be noticed by the target audience and not lost in the 'noise' of other messages. The audience must then comprehend the message so it should be presented in a way that is understandable to that audience. The audience must then accept the message, which means that it must fit into their worldviews. The message should have a length of retention that enables it to be translated from the cognitive domain into behavioural change (Cragin and Gerwehr, 2005). Each of these stages needs to be successful to obtain the three outcomes listed in Figure 2. The success of the radical Islamists in the last decade is that they have achieved all three stages in some form or another, by a concerted information operations effort that has involved targeted violence that has symbolic significance to both friend and foe They have not only managed to create a global movement from a small number of people, but to convert a significant number of others to their cause.

NEW TECHNOLOGY AND INFLUENCE

The development of the Internet, mobile technologies, and global communications has enabled many terrorist groups to access cheap means to send their messages to the world. Whilst terrorists use the Internet for instrumental purposes such as fundraising and command and control, there is now the capability to perform psychological and propaganda operations on a scale not available until the mid-1990s. As Weinman (2004, 2006) states; the Internet offers, easy access, anonymity, a global audience, low cost presence, a relatively uncensored environment, an ability to by-pass the formal mass media, and a presentation capability from multimedia products to achieve a strong impact.

Almost all terrorist organisations have a Web presence – even the technologically averse Taliban. The sites promote their cause in the best light as any other government or commercial site would do. Each is designed to present to and, sometimes mobilise, current and potential supporters as well as public opinion their view of the world and to promote their agenda.

Other innovations such as 'Captology' (Fogg, 2003) will enable all Web users to exploit the influencing potential of Web sites and their associated multimedia content. (Captology is an acronym based on the phrase *computers and persuasive technologies*). It aims to use design to further behaviour and attitude change, compliance motivation, and changes in worldview (*ibid*, p.5) .Whilst this is still at an early stage, this new design emphasis might have high potential to government, industry and terrorist organisations. Whilst Captology is limited to conventional computers presentation, other technologies such as mobile devices will become vulnerable to influence campaigns.

CONCLUSION

Information terrorism has many components from cyber-terrorism (or the threat of cyber-terrorism – *cyber-fear*), to command and control to psychological operations. This paper has outlined the function of influence in this mix. Of course, each component is an integral part of the other. For instance, the use of cyber-fear could be used in an influence campaign as a coercive tool. It is interesting to observe that the skills needed to run effective public relations campaigns in 'conventional' organisations has been exploited to the full by terrorist related groups to the point that it could be argued that they can control the mass media's agenda.

As the concept of information operations has matured, there has been increasing emphasis on the persuasive and influential components of information operations and less on the technological based concept of network wars. Both are still important but the 21st century has seen the concept of a 'mind war' come to the fore. Of course, this is nothing new as history is littered with examples of mind wars, for instance the French Wars of religion in the sixteenth century, which used the printing press as its tool, or the Cold War of the twentieth century, which used radio and television as its tools to promulgate ideas.

However, the ability to communicate globally and the development of psychological methods to coerce, influence or persuade has potentially increased their effectiveness. Terrorists know this and their aim is to sell

their ideas to achieve power or other goals. Whilst the conflict is asymmetric, with the military might in favour of the terrorists' enemies, then psychological warfare is their most effective option.

REFERENCES

Arquilla, J., Ronfeldt, D., Zanini, M. (1999) Networks, Netwar, and Information Age Terrorism, in: *Countering the New Terrorism*, RAND, Santa Monica, pp.39-84.

Cragin, K., Gerwehr, S. (2005) *Dissuading Terror: Strategic Influence and the Struggle Against Terrorism*, RAND, Santa Monica.

Fogg, B.J. (2003) *Persuasive Technology: Using Computers to Change What We Think and Do*, Morgan Kaufmann Publishers, San Francisco.

Goldstein, F.L., Jacobowitz, D.W. (1996) Psychological Operations: An Introduction, in: *Psychological Operations: Principles and Case Studies*, ed. F.L.Goldstein, Air University Press, Maxwell Airforce Base, Alabama, pp. 5-16.

Hall, W.M. (2003) *Stray Voltage: War in the Information Age*, Naval Institute Press, Maryland.

Hoffman, B, (1998) *Inside Terrorism*, Columbia University Press, New York.

Hoffman, B. (1999) Terrorism Trends and Prospects, in: *Countering the New Terrorism*, RAND, Santa Monica, pp.7-38.

Libicki, M.C. (1995) *What is Information Warfare?* National Defense University, Washington.

Medhurst, P. (2002) *Global Terrorism*, UNITAR, New York.

Tuman, J.S. (2003) *Communicating terror: The Rhetorical Dimensions of Terrorism*, Sage Publications, Thousand Oaks, CA.

Weimann, G. (2004) How Modern Terrorism Uses the Internet, United States Institute of Pease, URL: **WWW.USIP.ORG**, Accessed 19 Sep 2006.

Weimann, G. (2006) *Terror on the Internet: The New Arena, the New Challenges,* United States Institute of Peace press, Washington, D.C.

COPYRIGHT

William Hutchinson ©2006. The author assigns SCISSEC & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SCISSEC & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors